ABSTRACT

[0078] A method and architecture that enables consumers to computer data from multiple providers without jeopardizing consumer privacy interests or intellectual property rights of providers is disclosed. The architecture includes a trust server that mediates the conferral and revocation of trust relationships between the two parties. The method also employs programmable security coprocessors at vulnerable sites requiring protection, namely at the trust server and at each consumer. The architecture further reflects the specific requirements of coprocessors within consumer-side installations and their server-side counterparts. A single coprocessor within a client platform serves multiple providers by allocating to each of them a virtualized trusted computing environment for software execution and data manipulation. Since the tamper-resistance offered by client-side coprocessors is subject to more stringent economic pressures than that offered by server-side hardware security modules (HSMs), the architecture includes containment capabilities that prevent compromised coprocessors from causing damage disproportionate to their numbers.